

WHAT IS CLAIMED IS:

- 1               1. A method for seeding a random number generator, the
- 2               method comprising the steps of:
  - 3               (a) retrieving a first data block from a memory;
  - 4               (b) initially seeding the random number generator using said
  - 5               first data block as a seed;
  - 6               (c) retrieving a number generated by the random number
  - 7               generator;
  - 8               (d) mapping said number to a memory address in said
  - 9               memory using a mathematical function;
  - 10              (e) retrieving a successive data block from said memory
  - 11              address; and
  - 12              (f) successively seeding the random number generator with a
  - 13              combination of said seed and said successive data block such that said
  - 14              combination of said seed and said successive data block becomes a resulting
  - 15              seed.

- 1               2. The method recited in claim 1, further comprising the
- 2               further step of:
  - 3               (e') after each performance of (e), testing for satisfaction of at
  - 4               least one criterion and if said at least one criterion is not satisfied, repeating (c),

5 (d), (e), and (e').

1               3.     The method recited in claim 2, wherein a criterion of said  
2     at least one criterion is an absence of a string of identical bits in said successive  
3     data block longer than a specified number of bits.

1               4.     The method recited in claim 3, wherein said specified  
2     number is equal to the number of bits in said successive data block.

1               5.     The method recited in claim 2, further comprising the  
2     further step of:

3               (e'') after each performance of (e'), checking the number of  
4     repetitions of (c), (d), (e), and (e') due to failure to satisfy said at least one  
5     criterion and stopping said repetitions when a specified number of said  
6     repetitions have been performed.

1               6.     The method recited in claim 5, wherein said specified  
2     number of said repetitions is two.

1               7.     The method recited in claim 1, wherein said first data  
2     block includes an identifier unique to a specified computer device.

1                   8.     The method recited in claim 1, wherein said first data  
2     block includes previously saved data.

1                   9.     The method of claim 1, wherein said mathematical  
2     function used in said mapping is:

3                    $f(x) = x \pmod{m} + b$        for  $x < b$ ;

4                    $f(x) = x$                           for  $b \leq x \leq b + m$ ; and

5                    $f(x) = x \pmod{m} + b$        for  $x > b + m$ ;

6                   wherein  $f(x)$  = said memory address to which said generated  
7     number is mapped;

8                    $x$  = retrieved number generated by random number generator;

9                    $b$  = base memory address; and

10                   $m$  = memory size.

1                   10.    The method recited in claim 1, wherein said combination  
2     of said seed and said successive data block is accomplished by hashing said  
3     seed and said successive data block.

1                   11.    An apparatus for seeding a random number generator, the  
2     apparatus comprising:

3                   a memory; and  
4                   a processor operatively coupled to said memory, wherein said  
5   processor is programmed to:

- 6                   (a)    retrieve a first data block from said memory;
- 7                   (b)    initially seed the random number generator using  
8                        said first data block as a seed;
- 9                   (c)    retrieve a number generated by the random number  
10                  generator;
- 11                  (d)    map said number to a memory address in said  
12                  memory using a mathematical function;
- 13                  (e)    retrieve a successive data block from said memory  
14                  address; and
- 15                  (f)    successively seed the random number generator  
16                  with a combination of said seed and said successive  
17                  data. block such that said combination of said seed  
18                  and said successive data block becomes a resulting  
19                  seed.

1                   12.    The apparatus recited in claim 11, wherein said processor  
2   is further programmed to:  
3                   (e')    after each performance of (e), test for satisfaction of at

4       least one criterion and if said at least one criterion is not satisfied, repeat (c),  
5       (d), (e), and (e').

1                   13.      The apparatus recited in claim 12, wherein said processor  
2    is further programmed to:

3                   (e'') after each performance of (e'), check the number of  
4    repetitions of (c), (d), (e), and (e') due to failure to satisfy said at least one  
5    criterion and stop said repetitions when a specified number of said repetitions  
6    have been performed.

1                   14.      An apparatus for seeding a random number generator, the  
2    apparatus comprising:

3                   (a)     means for retrieving a first data block from a memory;  
4                   (b)     means for initially seeding the random number generator  
5    using said first data block as a seed;

6                   (c)     means for retrieving a number generated by the random  
7    number generator;

8                   (d)     means for mapping said number to a memory address in  
9    said memory using a mathematical function;

10                  (e)     means for retrieving a successive data block from said  
11   memory address; and

12 (f) means for successively seeding the random number  
13 generator with a combination of said seed and said successive data block such  
14 that said combination of said seed and said successive data block becomes a  
15 resulting seed.

1                   15. The apparatus recited in claim 14, further comprising:  
2                   (e') means for testing for satisfaction of at least one criterion  
3 after each use of said means for said retrieving said successive data block of  
4 (e), and if said at least one criterion is not satisfied, repeating (c), (d), (e), and  
5 (e').

1                    16. The apparatus recited in claim 15, further comprising:  
2                    (e'') means for checking the number of repetitions of (c), (d),  
3 (e), and (e') due to failure to satisfy said at least one criterion after each use of  
4 said means for said testing and repeating of (e'), and stopping said repeating  
5 when a specified number of said repetitions have been performed.

1               17. A computer-readable medium having computer-readable  
2 instructions for performing a method of accessing a database of interest, the  
3 method comprising the steps of:  
4               (a) retrieving a first data block from a memory;  
5               (b) initially seeding the random number generator using said  
6 first data block as a seed;  
7               (c) retrieving a number generated by the random number  
8 generator;  
9               (d) mapping said number to a memory address in said  
10 memory using a mathematical function;  
11              (e) retrieving a successive data block from said memory  
12 address; and  
13              (f) successively seeding the random number generator with a  
14 combination of said seed and said successive data block such that said  
15 combination of said seed and said successive data block becomes a resulting  
16 seed.

1               18. The computer-readable medium recited in claim 17,  
2 wherein said method further comprises the further step of:  
3              (e') after each performance of (e), testing for satisfaction of at

4 least one criterion and if said at least one criterion is not satisfied, repeating (c),  
5 (d), (e), and (e').

1                   19. The computer-readable medium recited in claim 18,

2 wherein said method further comprises the further step of:

3                   (e'') after each performance of (e'), checking the number of  
4 repetitions of (c), (d), (e), and (e') due to failure to satisfy said at least one  
5 criterion and stopping said repetitions when a specified number of said  
6 repetitions have been performed.